National Infrastructure Protection Center
CyberNotes

Issue #2001-12 *June 18, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between June 2 and June 14, 2001. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Group[1]	MacOS X 10.0, 10.0.1, 10.0.2, 10.0.3	Apache 1.3.14 Mac	A vulnerability exists when the Apache webserver is used with Mac OS X Client, which could let a remote malicious user gain sensitive information.	The vendor has addressed this problem in the Mac OS X Server, so it is advisable to run this OS if you plan on running a production webserver. Running Mac OS X Client under the UFS filesystem will also resolve this issue.	MacOS X Client Apache File Protection Bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[1] Bugtraq, June 10, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Caldera International, Inc. [2]	Unix	Volution 1.0, 1.0.6, 1.0.7	A vulnerability exists in the client authentication of Volution, which could let a malicious user gain full administrative access to the system.	Upgrade available at: ftp://ftp.caldera.com/pub/updates/Volution/1.0/current/RPMS/csm-1.0.8-47.i386.rpm	Volution Client Authentication Failure Hijacking	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
CG Information [3]	Windows 95/98/ME/ NT 4.0/2000	BiblioWeb 2.0	A remote Denial of Service vulnerability exists when a long URL is submitted.	No workaround or patch available at time of publishing.	BiblioWeb Long URL Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
cgiCentral[4]	Multiple	WebStore 400CS 4.14, 400 4.14	Two vulnerabilities exist: a vulnerability in the way ws_mail.cgi filters metacharacters out of the user-supplied data; and the ws_mail.cgi script unsafely passes user-submitted data to the 'system' command, which could let a malicious user execute arbitrary commands and gain administrative access.	No workaround or patch available at time of publishing.	WebStore Arbitrary Command Execution and Administrator Authentication Bypass	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Cicso Systems[5]	Multiple	Cisco 6400 NRP2 12.1DC	A vulnerability exists because the Access Concentrator NRP2 module allows Telnet access when no password is set, which could let a remote malicious user gain access to secure systems.	Upgrade available at: http://www.cisco.com.	Cisco NRP2 Unauthorized Telnet Access	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Evolvable Corporation[6]	Windows NT	Shambala 4.5	A directory traversal vulnerability exists in the 'CWD' command, which could let a remote malicious user gain sensitive information.	No workaround or patch available at time of publishing.	Shambala FTP Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Hewlett Packard[7]	Unix	OpenView Network Node Manager 5.01, 6.1	A vulnerability exists in the default configuration of the daemon, which could let a remote malicious user execute commands on a NNM managed system with the privileges of user bin.	Patch available at http://us-support2.external.hp.com/wpsl/bin/doc.pl	OpenView Network Node Manager SNMPNotify Command Execution	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Hewlett-Packard[8]	Unix	HP-UX 11.0	A symbolic link vulnerability exists in kmmodreg, which could let a malicious user overwrite arbitrary files or possibly gain elevated privileges.	Patch available at: PHCO_24112 http://us-support.external.hp.com/common/bin/doc.pl/distrib_redir=0991759980|*	HP-UX kmmodreg Symbolic Link	Medium	Bug discussed in newsgroups and websites. There is no exploit required.

[2] Caldera Security Advisory, CSSA-2001-021.0, June 8, 2001.
[3] Securiteam, June 13, 2001.
[4] Securiteam, June 13, 2001.
[5] Cisco Security Advisory, CI-01.07, June 14, 2001.
[6] Securiteam, June 7, 2001.
[7] Bugtraq, June 11, 2001.
[8] Bugtraq, June 4, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Jetico[9]	Unix	BestCrypt 0.7	A vulnerability exists in the 'bctool' command-line interface program, which could let a malicious user execute arbitrary code with root privileges.	Upgrade available at: http://www.jetico.com/download.htm	BestCrypt Arbitrary Privileged Program Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit required.
Jetico[10]	Unix	BestCrypt 0.6, 0.7, 0.8-1	A vulnerability exists due to insufficient bounds checking by 'bctool' when unmounting an encrypted file, which could let a malicious user gain elevated privileges. This could lead to execution of code as root.	Upgrade available at: http://www.jetico.com/download.htm	BestCrypt BCTool UMount Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Marty Bochane[11]	Unix	MDBMS 0.96b6, 0.99b4-0.99b6, 0.99b9	A buffer overflow vulnerability exists in the way the '\s' console command is handled, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.hinttech.com/mdbms/tar/mdbms1.0.source.tar.gz	MDBMS Query Display Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Maxum Development Corporation[12]	Mac OS (9.x and earlier)	Maxum Rumpus FTP Server 1.3.2- 1.3.5, 2.0.3dev	A Denial of Service vulnerability exists when a directory is created with an unusually large number of subfolders.	Upgrade available at: http://www.maxum.com/Upgrades/	Rumpus FTP Server Stack Overflow Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[13]	Windows 2000	Windows 2000 Datacenter Server SP1&SP2; 2000 Advanced Server SP1&SP2; Datacenter Server; 2000 Professional SP1&SP2; 2000 Server SP1&SP2	Four Denial of Service vulnerabilities exist: 1) The possibility of preventing an idle Telnet session from timing out. 2) A handle leak occurrence when a Telnet session is terminated in a certain way. 3) An access violation in the Telnet service caused by a logon command containing a particular malformation. 4) The effect of terminating a Telnet session caused by a system call, using only normal user privileges.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-031.asp	Microsoft Windows 2000 Denial of Service Vulnerabilities CVE Names: CAN-2001-0345, CAN-2001-0346, CAN-2001-0348, CAN-2001-0351	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[9] Securiteam, June 5, 2001.
[10] Bugtraq, June 14, 2001.
[11] Bugtraq, June 12, 2001.
[12] Bugtraq, June 12, 2001.
[13] Microsoft Security Bulletin, MS01-031, June 7, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[14]	Windows 2000	Windows 2000 Datacenter Server SP1&SP2; 2000 Advanced Server SP1&SP2; Datacenter Server; 2000 Professional SP1&SP2; 2000 Server SP1&SP2	Two vulnerabilities exist due to the way the Telnet service handles server-side named pipes, which could let a malicious user elevate privileges and gain full control over an affected server.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-031.asp	Microsoft Windows 2000 Privilege Elevation Vulnerabilities CVE NAMES: CAN-2001-0349, CAN-2001-0350	**High**	Bug discussed in newsgroups and websites.
Microsoft[15]	Windows 2000	Windows 2000 Datacenter Server SP1&SP2; 2000 Advanced Server SP1&SP2; Datacenter Server; 2000 Professional SP1&SP2; 2000 Server SP1&SP2	An information disclosure vulnerability exists if a userid is specified in a particular way when a user logs onto an affected Telnet server, which could let a malicious user find Guest accounts exposed via the Telnet server.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-031.asp	Microsoft Windows 2000 Information Disclosure CVE Name: CAN-2001-0347	Medium	Bug discussed in newsgroups and websites.
Microsoft[16]	Windows 95/98/NT 4.0/2000	Internet Explorer 5.0, 5.01 SP1 & SP2, 5.5, 5.5SP1	A vulnerability exists if a known local file on the client filesystem is referenced as a script source, which could allow a malicious website operator to obtain data from a visiting user's system.	No workaround or patch available at time of publishing.	Microsoft Internet Explorer File Contents Disclosure	Medium	Bug discussed in newsgroups and websites.

[14] Microsoft Security Bulletin, MS01-031, June 7, 2001.
[15] Microsoft Security Bulletin, MS01-031, June 7, 2001.
[16] Bugtraq, June 6, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[17]	Windows 98/98/ME/ NT 4.0/2000; Mac OS (9.x and earlier)	Microsoft Outlook Express for MacOS 4.5, 5.0; Outlook Express 4.0, 4.01, 4.27.3110.1, 4.72.2106.4, 4.72.3120.0, 4.72.3612. 1700, 5.0, 5.0.1, 5.5; Outlook 97/98/2000	A vulnerability exists which could let a remote malicious user cause messages written for one email address to be delivered to another email address (even though the spoofed address is displayed).	Workaround: Disable the "Automatically put people I reply to in my address book" option of Outlook Express.	Microsoft Outlook Express Address Book Spoofing	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[18]	Windows NT 4.0/2000	Exchange Server 2000, Server 5.5, 5.5 SP1-SP4	A vulnerability exists due to the interaction between Outlook Web Access (OWA) and Internet Explorer, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-030.asp	Microsoft Exchange OWA Embedded Script Execution CVE Name: CAN-2001-0340	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft[19]	Windows NT 4.0/2000	SQL Server 7.0, SQL Server 2000 Gold	One SQL query method contains a vulnerability that makes it possible for one user's query to reuse a cached connection that belonged to the sa account. This could allow a malicious user to access the database with administrative privileges.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-032.asp	Microsoft SQL Server Administrator Cached Connection CVE Name: CAN-2001-0344	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Multiple Vendors[20]	Unix	XFree86 xfs 4.0.1, 4.0.3	A Denial of Service vulnerability exists in the X font server (xfs) when connections are made numerous times and random data is sent.	No workaround or patch available at time of publishing.	XFree86 xfs Denial of Service	Low	Bug discussed in newsgroups and websites. No exploit is required.
Multiple Vendors[21]	Unix	RedHat Linux 6.1-6.2, 7.0-7.1; Debian Linux 2.1-2.3	A vulnerability exists in the 'man' system manual pager program, which could let a malicious user elevate their privileges.	No workaround or patch available at time of publishing.	Linux Man Malicious Cache File Creation	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[17] Securiteam, June 8, 2001.
[18] Microsoft Security Bulletin, MS01-030 (version 3.0), June 13, 2001.
[19] Microsoft Security Bulletin, MS01-032, June 12, 2001.
[20] Bugtraq, June 6, 2001.
[21] Securiteam, June 5, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[22]	Unix	NetBSD 1.4.1, 1.4.2, 1.4.3, 1.5; OpenBSD 2.8, 2.9	A race condition vulnerability exists in some ptrace implementations, which could let a malicious user elevate their privileges.	**NetBSD:** NetBSD has fixed this vulnerability in their main source tree, but has not released official fixes or a new kernel version. Administrators may install a snapshot or download diffs from the NetBSD cvs server at: http://cvsweb.netbsd.org/bsdweb.cgi/ **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patches/	Multiple BSD Vendor Ptrace Race Condition	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[23]	Unix	Patrick Powell LPRng 3.6.1, 3.6.10-3.6.19, 3.6.2, 3.6.20, 3.6.3-3.6.9, 3.7.4	A vulnerability exists when the LPRng daemon is initialized, which could let a malicious user elevate privileges.	**RedHat:** ftp://updates.redhat.com/7.0/en/os/	LPRng Failure To Drop Supplementary Groups	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[24]	Unix	Xinetd 2.1.8.8, 2.1.8.9pre1-2.1.8.9 pre15, 2.1.8.9pre2-2.1.8.9pre9	A buffer overflow vulnerability exists in the xinetd daemon, which could let a remote malicious user execute arbitrary code and gain root privileges.	**RedHat:** ftp://updates.redhat.com/7.1/en/os/i386/xinetd-2.1.8.9pre15-2.i386.rpm	Xinetd Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[22] Georgi Guninski Security Advisory #47, June 14, 2001.
[23] Red Hat Security Advisory, RHSA-2001:077-05, June 11, 2001.
[24] Securiteam, June 13, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[25, 26, 27, 28] ***Exploit Script released***[29]	**Unix**	**Linux-Mandrake 7.1, 7.2, Corporate Server 1.0.1; Immunix OS 7.0-beta and 7.0; Conectiva Linux 4.0, 4.0es, 4.1, 4.2, 5.0, prg gráficos, ecommerce, 5.1, 6.0; Debian GNU/Linux 2.2; Slackware 7.1, current**	**A buffer overflow vulnerability exists in the sudo program, which could let a malicious user gain root privileges.**	**Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3 **Immunix:** http://immunix.org/ImmunixOS/7.0/updates/RPMS/sudo-1.6.3p6-1_imnx_1.i386.rpm **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/dists/stable/updates/ **Slackware:** ftp://ftp.slackware.com/pub/slackware/	**Sudo Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***
O'Reilly Software[30]	Windows 98/98/NT 4.0	WebBoard 4.10.30	A vulnerability exists which could let a remote malicious user compose a message in the interactive messaging function that contains JavaScript code. This would be executed without asking the user.	No workaround or patch available at time of publishing.	WebBoard Pager Hostile JavaScript	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
OpenBSD[31]	Unix	OpenBSD 2.6-2.9	A Denial of Service vulnerability exists due to a design problem, which can allow a file descriptor of a process to drop into sleep while another process sharing the same file descriptor table sets the file descriptor to null.	No workaround or patch available at time of publishing.	OpenBSD Pipe and Dup2 VFS Race Conditions Denial Of Service	Low	Bug discussed in newsgroups and websites.
OpenBSD[32]	Unix	OpenSSH 2.2.0, 2.1.1, 2.3.1, 2.5.2, 2.5.2p2	A vulnerability exists when connecting to a system over ssh and using X11 forwarding, which could let a malicious user arbitrarily delete a cookie file belonging to another user.	No workaround or patch available at time of publishing.	OpenSSH Client X11 Forwarding Cookie Removal File Symbolic Link	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Packet Knights[33]	Unix	FPF Linux Kernel Module 1.0	A Denial of Service vulnerability exists when fragmented packets are sent to a machine with the FPF module loaded.	Upgrade available at: http://www.pkcrew.org/tools.php	Linux FPF Kernel Module Denial Of Service	Low	Bug discussed in newsgroups and websites. This can be exploited using nmap.

[25] Linux-Mandrake Security Update Advisory, MDKSA-2001:024, February 26, 2001.
[26] Immunix OS Security Advisory, IMNX-2001-70-004-01, February 26, 2001.
[27] Conectiva Linux Security Announcement, CLA-2001:381, February 26, 2001.
[28] Debian Security Advisory, DSA-031-2, March 6, 2001.
[29] Synnergy Networks, June 6, 2001.
[30] Securiteam, June 7, 2001.
[31] Bugtraq, June 2, 2001.
[32] Bugtraq, June 5, 2001.
[33] Bugtraq, June 2, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PassWD[34]	Windows 95/98/ME/ NT 4.0/2000	PassWD 2000 2.0, 2.5-2.8	A vulnerability exists because the session key is encoded using a fixed master key, which could let a malicious user break the algorithm and gain access to all login information.	The vendor is reportedly not supporting this product anymore.	PassWD 2000 Weak Password Encryption	Medium	Bug discussed in newsgroups and websites.
PKCrew[35]	Unix	TIATunnel 0.9alpha2, 0.9alpha3	A buffer overflow vulnerability exists in the authentication mechanism, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://tiatunnel.pkcrew.org/download/tiatunnel-0.9alpha3.tar.gz	TIATunnel Authentication Mechanism Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Pragma Systems[36]	Windows 95/98/NT 4.0	InterAccess TelnetD Server 4.0, 4.0 Build 4 & 5	A Denial of Service vulnerability exists if large bursts of data are sent to port 23 (Telnet).	Upgrade available at: http://www.pragmasys.com/Downloads.html	InterAccess Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Qualcomm[37]	Multiple	qpopper 4.0-4.0.2	A buffer overflow vulnerability exists in the qpopper source tree, which could let a remote malicious user gain root privileges.	Upgrade available at: ftp://ftp.qualcomm.com/eudora/servers/unix/popper/qpopper4.0.3.tar.gz	qpopper Username Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
RedHat[38]	Unix	Linux 6.1, 6.2, 7.0, 7.1	A buffer overflow vulnerability exists in the implementation of the 'man' system manual pager program, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Linux Man Page Source Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
RedHat[39]	Unix	Linux 7.0 alpha, i386, 7.1 i386	A vulnerability exists in the xinetd daemon, which could let a malicious user create world-writable files.	Upgrade available at: ftp://updates.redhat.com/	Xinetd Insecure Default Umask	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
RedHat[40]	Unix	Ken Stevens ispell 3.1.20	A vulnerability exists in versions of ispell due to the way gnomerpm handles tmp files, which could let a malicious user create or overwrite files.	Upgrade available at: ftp://updates.redhat.com/	Ken Stevens ispell Symbolic Link	Medium	Bug discussed in newsgroups and websites.
SCO[41]	Unix	Unixware 7.0- 7.1.1	A buffer overflow vulnerability exists in the implementation of libtermcap used by Unixware, which could let a malicious user elevate their privileges.	No patch or patch available at time of publishing.	Unixware Libtermcap Buffer Overflow	Medium	Bug discussed in newsgroups and websites.

[34] Bugtraq, June 4, 2001.
[35] Qitest1's Security Advisory #001, June 6, 2001.
[36] Bugtraq, June 6, 2001.
[37] Bugtraq, June 2, 2001.
[38] Bugtraq, June 12, 2001.
[39] Red Hat Security Advisory, RHSA-2001:075-04, June 5, 2001.
[40] Red Hat Security Advisory, RHSA-2001:074-03, June 4, 2001.
[41] Bugtraq, June 11, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Screaming Media, Inc.[42]	Multiple	SiteWare 2.5, 2.501, 3.0, 3.01, 3.02, 3.1	Two vulnerabilities exist: a source code disclosure vulnerability; and a directory traversal vulnerability exists which could let a remote malicious user gain sensitive information.	In order to obtain the upgrade, contact the vendor at: support@screamingmedia.com	SiteWare Source Code and Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Source Forge[43]	Unix	kosch suid wrapper 1.1.1	A buffer overflow vulnerability exists in the suid wrapper, which could let a malicious user execute arbitrary code/commands.	No workaround or patch available at time of publishing.	Suid Wrapper Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Sun Micro-Systems, Inc.[44]	Unix	Solaris 8.0_x86	A buffer overflow vulnerability exists in /usr/bin/mail, which could let a malicious user execute arbitrary code/commands.	No workaround or patch available at time of publishing.	Solaris Mail HOME Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Thibault Godouet[45]	Unix	FCron 1.0, 1.0.1-1.0.3, 1.1.0	A symbolic link vulnerability exists in the fcron template, which could let a malicious user corrupt another user's crontab file, interfering with scheduled events and potentially creating a Denial of Service.	No workaround or patch available at time of publishing.	Fcron Symbolic Link	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
TransSoft[46]	Windows 95/98/ME/ NT 4.0/2000	Broker FTP Server 4.0, 4.7.5.0, 5.0, 5.1, 5.7, 5.9.5	Two vulnerabilities exist: a directory traversal vulnerability exists, which could let a remote malicious user gain sensitive information; and a buffer overflow vulnerability in the CWD command, which could let a malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	Broker FTP Server Directory Traversal and CWD Buffer Overflow Vulnerabilities	Low/ Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Trend Micro, Inc.[47]	Windows NT 3.5/3.5.1/ 4.0	InterScan VirusWall for Windows NT 3.51	A vulnerability exists in the administrator functions, which could let a remote malicious user improperly gain access to admin functions.	No workaround or patch available at time of publishing.	InterScan VirusWall Configurations Modification	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Trend Micro, Inc.[48]	Windows NT 3.5/3.5.1/ 4.0	InterScan VirusWall for Windows NT 3.51	A buffer overflow vulnerability exists in the administrative programs, FtpSaveCSP.dll and FtpSaveCVP.dll, which could let a remote malicious user gain system privileges and execute arbitrary code.	No workaround or patch available at time of publishing.	InterScan VirusWall Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[42] Foundstone Security Advisory, FS-061201-19-SMSW, June 11, 2001.
[43] Securiteam, June 9, 2001.
[44] Georgi Guninski Security Advisory #46, June 4, 2001.
[45] Bugtraq, June 7, 2001.
[46] Bugtraq, June 10, 2001.
[47] SNS Advisory No.30, June 12, 2001.
[48] SNS Advisory No.31, June 13, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Trend Micro, Inc.[49]	Windows NT 4.0/2000	Virus Control System 1.8	An authentication vulnerability exists in the CGI script, which could let a remote malicious user gain access to administrative programs and data without authentication.	No workaround or patch available at time of publishing.	Virus Control System Admin Script Authentication Bypass	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
University of Cambridge [50]	Unix	Exim 3.11-3.22	A format string vulnerability exists, which could let a remote malicious user execute arbitrary code with root privileges. This vulnerability exists only when the 'syntax checking' mode is turned on, which is not by default.	**Debian:** http://security.debian.org/dists/stable/updates/main/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/6.0	Exim Format String	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
University of Washing-ton[51]	Unix	imapd 2000a, 2000b, 2000c	Several buffer overflow vulnerabilities exist, which could let a malicious user elevate their privileges.	**MandrakeSoft:** ftp://ftp.planetmirror.com/raid/6/mandrake/updates/	Imapd 'Local' Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Watch Guard[52]	Multiple	Firebox 4500 4.5, 4.6; Firebox 2500 4.5, 4.6	A vulnerability exists in the firewall due to the way attachments are encoded, which could let a remote malicious user send attachments such as functional VB scripts in email, and bypass filtering at the firewall.	No workaround or patch available at time of publishing.	Firebox SMTP Proxy Attachment Bypassing	Medium/ **High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites. Exploit has been published.
WebTrends [53]	Windows NT	WebTrends Enterprise Reporting Server 3.1c, NT 3.5	A vulnerability exists when a URL is crafted with an encoded space after the filename of the script, which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	WebTrends Reporting Server Script Source Code Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit required.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such a vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of a medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. It should be noted that while the DoS

[49] Secure Net Service Advisory No.29, June 7, 2001.
[50] Debian Security Advisory, DSA-058-1, June 10, 2001.
[51] Mandrake Linux Security Update Advisory, MDKSA-2001:054, June 10, 2001.
[52] Securiteam, June 11, 2001.
[53] Bugtraq, June 3, 2001.

attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between June 4 and June 13, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 25 scripts, programs, and net-news messages containing holes or exploits were identified. *At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
June 14, 2001	Bcexp.c	Script which exploits the BestCrypt BCTool UMount Buffer Overflow vulnerability.
June 14, 2001	Vvopenbsd.c	Script which exploits the Multiple BSD Vendor Ptrace Race Condition Vulnerability.
June 13, 2001	**Webstorekill.pl**	**Perl script which exploits the WebStore Arbitrary Command Execution and Administrator Authentication Bypass vulnerabilities.**
June 12, 2001	**Man-1.5i-4-root-exploit.tar.gz**	**Exploit script for the Linux Man Page Source Buffer Overflow vulnerability.**
June 12, 2001	Mdbms.tar.gz	Exploit for the MDBMS Query Display Buffer Overflow vulnerability.
June 10, 2001	**Brokerdos.pl**	**Perl script which exploits the TransSoft Broker FTP Server Directory Traversal and CWD Buffer Overflow Vulnerabilities.**
June 8, 2001	Adv_mstelnet.txt	Perl exploit for the Microsoft Windows 2000 Telnet vulnerability.
June 8, 2001	Openview.snmp.txt	Exploit details for the OpenView Network Node Manager SNMPNotify Command Execution vulnerability.
June 7, 2001	**Mandebian.sh**	**Exploit for the Debian Linux Man Malicious Cache File Creation vulnerability.**
June 7, 2001	**Manredhat.sh**	**Exploit for the RedHat Linux Man Malicious Cache File Creation vulnerability.**
June 7, 2001	Mstelnettest.sh	Exploit for the Windows 2000 Denial of Service Vulnerability.
June 7, 2001	Passlogd-0.1c.tar.gz	A sniffer which logs traffic on the UDP syslog port.
June 7, 2001	**Su-wrapper.c**	**Script which exploits the Suid Wrapper Buffer Overflow vulnerability.**
June 6, 2001	**Alt3kx-advisories-2001.txt**	**Exploit technique for the QVT/NET 4.3 FTP Server and the Shambala FTP Server vulnerabilities.**
June 6, 2001	Flawfinder-0.15.tar.gz	Flawfinder searches through source code for potential security flaws, listing potential security flaws sorted by risk, with the most potentially dangerous flaws shown first.
June 6, 2001	Iatunauth-ex.c	Script which exploits the TIATunnel Authentication Mechanism Buffer Overflow vulnerability.
June 6, 2001	Pragma.pl	Perl script which exploits the Pragma InterAccess Denial of Service vulnerability.
June 6, 2001	Tiatunnel.c	Script which exploits the TIATunnel Authentication Mechanism Buffer Overflow vulnerability.
June 6, 2001	Vudo.c	Script which exploits the Sudo-1.6.3p5 Buffer Overflow Vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
June 5, 2001	ICMP_Scanning_v3.0.zip	Paper that outlines what can be done with the ICMP protocol regarding scanning and includes details on host detection techniques, inverse mapping, trace routing, OS fingerprinting methods with ICMP, and which ICMP traffic should be filtered on a filtering device.
June 5, 2001	Stealth-syscall.txt	An article that describes a technique of redirecting system calls without modifying the sys call table (implemented in Linux). This can be used to evade intrusion detection systems that use the sys call table to register redirected or Trojaned system calls.
June 4, 2001	Mimedefang-1.2.tar.gz	A flexible MIME email scanner.
June 4, 2001	**Nmap-2.54BETA25.tgz**	**A utility for port scanning large networks.**
June 4, 2001	**Solmail.pl**	**Perl script which exploits the SunOS mail HOME Buffer Overflow vulnerability.**
June 4, 2001	**Sunhome.txt**	**Exploit for the SunOS 5.8 x86 Buffer Overflow vulnerability.**

Trends

Probes/Scans:

- **CERT/CC continues to observe increased network reconnaissance activity and a significant increase in the number of generalized port scans of hosts.**

Other:

- A worm called DoS.Storm.Worm seeks out Microsoft Internet Information Services (IIS) systems that have not applied the proper security patches. Any systems that the worm finds are then infected with the worm. The payload of this worm performs a Denial of Service attack on www.microsoft.com (See Virus Section).
- **The CERT/CC has received several inquiries about an email virus warning currently in circulation on the Internet. The email contains several language translations of a virus warning related to the file SULFNBK.EXE. This email message is a HOAX. Although the SULFNBK.EXE file may be infected by a number of valid viruses, the mere presence of the file as described in the message is not a sign of a virus infection. The SULFNBK.EXE file is a legitimate Microsoft Windows utility that is used to restore long file names.**
- Recent reports on IIS vulnerabilities and the large amount of NT servers being penetrated using different exploits have raised the need to tighten the security of IIS version 5.0 servers. Please see the IIS version 5.0 checklist at: http://www.microsoft.com/technet/security/iis5chk.asp.
- **CERT/CC has received reports of a new piece of self-propagating malicious code referred to as the sadmind/IIS worm. The worm uses two well-known vulnerabilities to compromise systems and deface web pages: A two-year-old buffer overflow vulnerability in the Solstice sadmind program; and after successfully compromising the Solaris systems, a seven-month-old vulnerability which compromises the IIS systems. For more information, please see CERT® Advisory CA-2001-11, located at: http://www.cert.org/advisories/CA-2001-11.html.**
- **There has been a very significant increase in attempts to exploit known weaknesses in the lpd/LPRng and RPC daemons (ports 515 and 111) of Unix-based operating systems. For more information, please see NIPC ALERT 01-010, located at: http://www.nipc.gov/warnings/alerts/2001/01-010.htm.**

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The following table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. NOTE: At times, viruses may contain names or content that may be considered offensive.

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Hybris	Worm	Slight Increase	November 2000
2	W32/Magistr	File, Worm	Slight Decrease	March 2001
3	PE_MTX.A	File Infector, Trojan	Slight Increase	September 2000
4	VBS/Homepage	Script	Slight Decrease	May 2001
5	W32/BadTrans	Worm	Slight Decrease	April 2001
6	VBS/Mawanella	Script	Slight Increase	May 2001
7	VBS/Kakworm	Script	Slight Increase	December 1999
8	VBS/Loveletter	Script	Slight Increase	March 2000
9	W32/Funlove	File	Decrease	November 1999
10	VBS/SST	Script, Worm	Return to Table	February 2001

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **221** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **476** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

AplS/Simpsons-A (Aliases: Mac.Simpson, MacSimpson, Mac/Simpsons@mm) (AppleScript Worm): This is the first AppleScript worm. AplS/Simpsons-A uses the scripting functionality of Outlook Express or Entourage to send itself via email to contacts in an infected user's address books. To mask its activity, the worm points Internet Explorer 5 to a website with information about the TV comedy show "The Simpsons." The worm arrives as an email with two attachments and the following text:

> "Hundreds of Simpsons episodes were just secretly produced and sent out on the Internet, if this message gets to you, the episodes are enclosed on the attachment program, which will only run on a Macintosh. You must have system 9.0 or 9.1 to watch the hilarious episodes, in high quality. Just download and open it.
> From, <name of the sender>"

The attached files are "Secret Simpsons Episodes!" and "Simpsons Episodes." The first file is a MIME copy of the email, and the second file contains the viral script. When the file is ran, it would place itself in the Startup Items folder in the System Folder in order to automatically run.

DoS.Storm.Worm (Worm): This is a worm that seeks out Microsoft Internet Information Services (IIS) systems that have not applied the proper security patches. When this worm is run, it sets up a server FTP thread and starts to scan 10,000,000 IP addresses in an attempt to find a vulnerable system at one of the targeted addresses. The vulnerable systems that it targets are Microsoft IIS installations (versions 4 and 5) that do not have the security patches installed to cover the "Web Server Folder Traversal" security vulnerability as described in http://www.microsoft.com/technet/security/bulletin/MS00-078.asp. Additional advice on securing IIS web servers is available from http://www.microsoft.com/technet/security/iis5chk.asp and http://www.microsoft.com/technet/security/tools.asp. When the worm finds a vulnerable system, it copies itself to the targeted system and sets it up to automatically run the worm, making that system a zombie that participates in the automated attacks. To make sure that the worm runs on the next system startup, the worm adds the value 666 C:\winnt\system32\storm\start.bat to the registry keys: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices and HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run. This worm has two payloads: A Denial of Service attack is initiated against http://www.microsoft.com, and an email bombing session is started that sends email messages containing an obscene message to gates@microsoft.com.

PE_HLLC.DANY.A (Aliases: Dany, HLLC.DANY.A, W32.HLLC.Danny, W32/Hamlet) (File Infector Virus): This virus is written in Microsoft Visual C++. Upon execution, it creates a copy of its target files and then infects all PE files with the .EXE extension in the current directory. The virus gives the copied files an .ISO file extension and overwrites the target files with its own code. A message box is then displayed containing an excerpt from the Shakespeare play "Hamlet."

JUDGE (Aliases: Judge.390, Judgement.390, Judgement Day, MP.390) (File Infector Virus): This non-destructive, memory-resident virus infects COM files. When the system day and date are Friday 13, it displays a message.

VBS.Catfish@mm (Visual Basic Script Worm): This is a Visual Basic Script worm. It arrives as Catfish.bat. This worm uses Microsoft Outlook, mIRC, and PIRCH to spread. Due to bugs in the code, this worm does not execute properly.

VBS.Lanus.gen (Visual Basic Script Worm): This is an encoded Visual Basic script (VBS) contained within a .htm or .html page. This script is viral, and when executed it infects .htm and .html files by appending itself to the end of the file. For the script to activate, you must have the Windows Scripting Host 5.1 or later installed and allow the ActiveX controls to run when the infected .htm or .html page is viewed.

VBS/Lovelet-CE (Visual Basic Script Worm): This is another variant of the VBS/Lovelet-A email-aware worm. The worm typically arrives in the form of an email with the following characteristics:

Subject line: News Email Beta Run1.01
Message text: News Matrix from http://go.to/ashop Test Run 1.01
Attached file: NEWSEMAIL.VBS

The worm copies itself to MSKERNEL32.VBS and NEWSEMAIL.VBS in the Windows System directory, and alters the Registry Run and RunServices keys to run these files on startup. It also copies itself to WIN32DLL.VBS in the Windows directory. The worm attempts to change the Internet Explorer start page, and if Outlook is installed, it will try to forward itself as an email attachment to addresses from the Outlook address book.

VBS_LOVELETTR.CN (Aliases: VBS_NAKEDBEACH.A, NAKEDBEACH.A, LOVELETTER.CM@MM, JENNIFERLOPEZ.WORM, LOVELETTR.CN) (VBS Script Worm): Upon execution, this destructive worm overwrites its codes to files with the extensions, .VBS, .VBE, .JS, .JSE, .CSS, .WSH, .SCT, .HTA, JPG, JPEG, .MP2, and .MP3. It uses Microsoft Outlook to send emails with a copy of itself as an attachment called "JENNIFERLOPEZ_NAKED.JPG.VBS" to all entries in an infected user's address book. This worm also drops and executes a CIH_14.EXE file. This file is infected with the destructive PE_CIH virus.

VBS.Nazburg.484 (Aliases: Nazburg.484, VBS/Nazburg.484) (Visual Basic Script Worm): This is a prepending Visual Basic script (VBS) virus. When executed, the script creates the files Nazburg.bat and Nazburg.com in the same folder as the virus. Nazburg.bat is executed, which in turn runs the Nazburg.com file. This searches for .vbs files in the current folder and adds 484 bytes of viral code to the beginning of any files that it finds. The batch file then deletes Nazburg.com.

VBS.Pando.A (Aliases: VBS.Pando, VBS/Pando) (Visual Basic Script Worm): This is an overwriting Visual Basic script (VBS) virus. It searches for .vbs files in the current folder (the location of the viral script), the parent folder of the current folder, and the Windows folder and then copies itself over these files. The script also creates the file 'Startup.lnk' in the StartUp folder. This shortcut ensures that the viral script is executed every time that Windows starts. If the current minute is :09 when the script is executed, a message will appear.

VBS.Pando.B (Aliases: VBS.Pando.b, VBS/Pando) (Visual Basic Script Worm): This is an overwriting Visual Basic script virus. It searches for .vbs files in the current folder (the location of the viral script) and the parent folder of the current folder, and overwrites these files with a copy of itself.

VBS.Reaper (Visual Basic Script Worm): This is a Visual Basic Script (VBS) worm that spreads using mIRC. It arrives as the file Christina_aguilera_nude!.vbs. When the script is run, the worm creates (or overwrites if it already exists) the file C:\Mirc\Script.ini, which is executed when mIRC is run. For this to happen, mIRC must be installed in the default location C:\Mirc. Once connected, two bogus "SECURITY WARNINGS" appear, prompting the user to input his nickname and password. It then sends this information to the script's creator. Finally, the worm sends itself to all other users in the channel as the file Christina_aguilera_nude!.vbs.

W32/Choke (Aliases: I-Worm.Choke, Win32.Choke, W32/Choke.Worm) (Win32 Worm): This virus has been reported in the wild. It is a worm which attempts to send itself through the MSN Messenger Instant Messaging program. The worm copies itself to c:\choke.exe and sets a Registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Choke in order to run automatically when Windows is started. When first executed the worm displays two dialog boxes. The first dialog box says: "This program needs Flash 6.5 to run!" The second displays the message: "Cannot run program!, Quitting." The worm creates a file called about.txt in the root of the C: drive.

W32/Themba (Aliases: W32.HLLP.Thembe (NAV) (Win32 Worm): This is an appending virus written in Visual Basic. When run, it infects all files in the current directory that contain the .EXE extension and other .EXE files that are run while an infected program is in loaded into memory.

W97M_INSPECTOR.A (Aliases: Macro.Word97.Inspector.b, W97M/Inspector.gen, INSPECTOR.A) (Word 97 Macro Virus): This macro virus infects Word documents only. It uses the auto macros AutoOpen, AutoClose, AutoExit, and AutoExec to execute. It has no destructive payload.

W97M_RECENT.A (Aliases: Macro.Word97.Recent, RECENT.A) (Word 97 Macro Virus): This macro virus infects Word documents upon close. It generates a random number between 1 and 31 and when this number equals the current system date, it displays a message box.

W97M.Soldier.A (Word 97 Macro Virus): This macro virus infects other open Microsoft Word documents when an infected document is opened. It also sends infected documents to two email addresses. W97M.Soldier.A also changes the Internet Explorer home page.

WM97/Myna-AR (Word 97 Macro Virus): WM97/Myna-AR is, like earlier family members, a Word macro virus that contains no intentionally malicious code. The replicating code contains the phrase MYNAMEISVIRUS, which is used as a flag to check for its presence.

WM97/Opey-AU (Word 97 Macro Virus): The virus removes the Macros section of the Tools menu and disables access to the Visual Basic Editor. It also changes the settings of File|Properties and Word User Information to include references to "eUgEnE" and "Ghostfighter Certified." The virus has five payloads, which trigger on different dates. During November, it displays a dialogue box with the message: "This Program is Possessed!!! Please answer the question to Access Program. (1) What do you call an irresponsible JI who shirks a duty or avoids work/obligation?" Giving the answer "slacker" or "slackers" will cause the virus to display "ACCESS GRANTED." Any other answer will cause "ACCESS DENIED" to be displayed, and the question to be displayed again. After three wrong answers the virus will close Word. On February 27 the virus will display the message "Happy B-DAY to ROSE MOLINA and MIRSA MERZA." On October 16 the message displayed will be "Welcome UERMMMC Medicine 2001 - OPD pipol!!! Especially to Master Joven, Tina and John, Peter, Seph, Slacker Henry MASIPAG na Ronnie, EVERFAITHFUL Agnes and lastly to the SUPER S Rose and Mirsa. Hello! din sa other half ng group (Mga S.O.L.'s) – Space Occupying Lesions. Hi! NETMI, pa-coffee naman kayo dyan =)." On October 3 the message will be "Happy Birthday to me! (The Author)." On July 27 the message says "Happy Birthday to my one and only Rica M."

WM97/Wrench-N (Word 97 Macro Virus): This is a variant of the WM97/Wrench-G Word macro virus. The virus contains some corrupted macros, which means the payload of displaying the Office Assistant does not work. The virus drops a file containing viral code called ASCII.VXD into the root directory.

XM97/Barisada-Y (Excel 97 Macro Virus): This is a variant of the XM97/Barisada Excel macro virus family that does not contain the common payload of displaying a series of message boxes. This virus creates the viral file KHM.XLS in the XLSTART directory, which it uses during replication.

XM97/Laroux-OC (Excel 97 Macro Virus): This variant of the XM97/Laroux family creates the viral file BINV.XLS in the XLSTART directory, which it uses to replicate.

Trojans

Trojan Horse programs have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are descriptions of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that their anti-virus software detects. *At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
Backdoor.Acropolis	N/A	CyberNotes-2001-04
Backdoor.Netbus.444051	N/A	CyberNotes-2001-04
Backdoor.NTHack	N/A	CyberNotes-2001-06
Backdoor.Quimera	N/A	CyberNotes-2001-06
Backdoor.SMBRelay	N/A	CyberNotes-2001-10
Backdoor.WLF	N/A	CyberNotes-2001-08
Backdoor-JZ	N/A	CyberNotes-2001-02
BAT.Black	N/A	CyberNotes-2001-11
BAT.Install.Trojan	N/A	CyberNotes-2001-04
BAT.Trojan.DeltreeY	N/A	CyberNotes-2001-07
BAT.Trojan.Tally	N/A	CyberNotes-2001-07
BAT_DELWIN.D	N/A	CyberNotes-2001-05
BAT_EXITWIN.A	N/A	CyberNotes-2001-01
BioNet	3.13	CyberNotes-2001-07
BSE Trojan	N/A	CyberNotes-2001-07

Trojan	Version	CyberNotes Issue #
DLer20.PWSTEAL	N/A	CyberNotes-2001-05
Eurosol	N/A	CyberNotes-2001-10
Fatal Connections	2.0	CyberNotes-2001-09
Flor	N/A	CyberNotes-2001-02
Freddy	beta 3	CyberNotes-2001-09
Gift	1.6.13	CyberNotes-2001-09
Goga	**N/A**	**Current Issue**
HardLock.618	N/A	CyberNotes-2001-04
Jammer Killah	1.2	CyberNotes-2001-10
JS.StartPage	N/A	CyberNotes-2001-07
Noob	4.0	CyberNotes-2001-09
PERL/WSFT-Exploit	N/A	CyberNotes-2001-11
PHP/Sysbat	N/A	CyberNotes-2001-02
PIF_LYS	N/A	CyberNotes-2001-02
PWSteal.Coced240b.Tro	N/A	CyberNotes-2001-04
SadCase.Trojan:	N/A	CyberNotes-2001-09
Scarab	1.2c	CyberNotes-2001-10
Troj/Futs	N/A	CyberNotes-2001-07
Troj/Keylog-C	N/A	CyberNotes-2001-08
Troj/KillCMOS-E	N/A	CyberNotes-2001-01
Troj/Unite-C	N/A	CyberNotes-2001-09
TROJ_AOL_EPEX	N/A	CyberNotes-2001-01
TROJ_AOLWAR.B	N/A	CyberNotes-2001-01
TROJ_AOLWAR.C	N/A	CyberNotes-2001-01
TROJ_APS.216576	N/A	CyberNotes-2001-03
TROJ_ASIT	N/A	CyberNotes-2001-07
TROJ_AZPR	N/A	CyberNotes-2001-01
TROJ_BADTRANS.A	N/A	CyberNotes-2001-08
TROJ_BAT2EXEC	N/A	CyberNotes-2001-01
TROJ_BCKDOR.G2.A	N/A	CyberNotes-2001-11
TROJ_BKDOOR.GQ	N/A	CyberNotes-2001-01
TROJ_BUSTERS	N/A	CyberNotes-2001-04
TROJ_CAINABEL151	1.51	CyberNotes-2001-06
TROJ_DARKFTP	N/A	CyberNotes-2001-03
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-05
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-04
TROJ_EUTH.152	N/A	CyberNotes-2001-08
TROJ_FIX.36864	N/A	CyberNotes-2001-03
TROJ_FUNNYFILE.A	N/A	CyberNotes-2001-09
TROJ_GLACE.A	N/A	CyberNotes-2001-01
TROJ_GNUTELMAN.A	N/A	CyberNotes-2001-05
TROJ_GOBLIN.A	N/A	CyberNotes-2001-03
TROJ_GTMINESXF.A	N/A	CyberNotes-2001-02
TROJ_HAVOCORE.A	N/A	CyberNotes-2001-09
TROJ_HERMES	N/A	CyberNotes-2001-03
TROJ_HFN	N/A	CyberNotes-2001-03
TROJ_ICQCRASH	N/A	CyberNotes-2001-02
TROJ_IDENTD.B	N/A	CyberNotes-2001-11
TROJ_IE_XPLOIT.A	N/A	CyberNotes-2001-08
TROJ_IF	N/A	CyberNotes-2001-05
TROJ_INCOMM16A.S	N/A	CyberNotes-2001-09
TROJ_JOINER.15	N/A	CyberNotes-2001-02
TROJ_JOINER.I	N/A	CyberNotes-2001-08
TROJ_LASTWORD.A	N/A	CyberNotes-2001-09
TROJ_LATINUS.SVR	**N/A**	**Current Issue**
TROJ_MATCHER.A	N/A	CyberNotes-2001-08
TROJ_MEGA.A	**N/A**	**Current Issue**

Trojan	Version	CyberNotes Issue #
TROJ_MOONPIE	N/A	CyberNotes-2001-04
TROJ_MOONPIE.A	N/A	CyberNotes-2001-11
TROJ_MSWORLD.A	**N/A**	**Current Issue**
TROJ_MTX.A.DLL	N/A	CyberNotes-2001-09
TROJ_MYBABYPIC.A	N/A	CyberNotes-2001-05
TROJ_NAKEDWIFE	N/A	CyberNotes-2001-05
TROJ_NARCISSUS.A	N/A	CyberNotes-2001-09
TROJ_NAVIDAD.E	N/A	CyberNotes-2001-01
TROJ_PARODY	N/A	CyberNotes-2001-05
TROJ_PICSHOW.A	N/A	CyberNotes-2001-10
TROJ_PORTSCAN	N/A	CyberNotes-2001-03
TROJ_Q2001	N/A	CyberNotes-2001-06
TROJ_QZAP.1026	N/A	CyberNotes-2001-01
TROJ_RUNNER.B	N/A	CyberNotes-2001-03
TROJ_RUX.30	N/A	CyberNotes-2001-03
TROJ_SCOUT.A	N/A	CyberNotes-2001-08
TROJ_SUB7.21.E	2.1	CyberNotes-2001-05
TROJ_SUB7.22.D	.22	CyberNotes-2001-06
TROJ_SUB7.401315	N/A	CyberNotes-2001-01
TROJ_SUB7.MUIE	N/A	CyberNotes-2001-01
TROJ_SUB7.V20	2.0	CyberNotes-2001-02
TROJ_SUB722	2.2	CyberNotes-2001-06
TROJ_SUB722_SIN	N/A	CyberNotes-2001-06
TROJ_SUB7DRPR.B	N/A	CyberNotes-2001-01
TROJ_SUB7DRPR.C	N/A	CyberNotes-2001-03
TROJ_TPS	N/A	CyberNotes-2001-05
TROJ_TWEAK	N/A	CyberNotes-2001-02
TROJ_VBSWG_2B	N/A	CyberNotes-2001-07
TROJ_WARHOME.A	**N/A**	**Current Issue**
TROJ_WEBCRACK	N/A	CyberNotes-2001-02
TROJ_WINMITE.10	N/A	CyberNotes-2001-08
Trojan.MircAbuser	N/A	CyberNotes-2001-04
Trojan.PSW.M2.14	N/A	CyberNotes-2001-07
Trojan.RASDialer	N/A	CyberNotes-2001-06
Trojan.Sheehy	N/A	CyberNotes-2001-05
Trojan.Taliban	N/A	CyberNotes-2001-07
Trojan.W32.FireKill	N/A	CyberNotes-2001-07
Trojan/PokeVB5	N/A	CyberNotes-2001-07
VBS.Cute.A	N/A	CyberNotes-2001-05
VBS.Delete.Trojan	N/A	CyberNotes-2001-04
VBS.Lumorg	N/A	CyberNotes-2001-09
VBS.Over.Trojan	N/A	CyberNotes-2001-10
VBS.Phybre	**N/A**	**Current Issue**
VBS.Reset	**N/A**	**Current Issue**
VBS.SystemColor.A	N/A	CyberNotes-2001-11
VBS.Trojan.Noob	N/A	CyberNotes-2001-04
VBS.Zeichen.A	N/A	CyberNotes-2001-08
VBS_HAPTIME.A	N/A	CyberNotes-2001-09
VBS_IESTART.A	N/A	CyberNotes-2001-11
W32.BatmanTroj	N/A	CyberNotes-2001-04
W32.BrainProtect	N/A	CyberNotes-2001-07
Y3K Rat	1.6	CyberNotes-2001-11

Goga: This Trojan has been reported in the wild. It steals and sends out from infected computers user details for Internet access (i.e., login, password and other information). It has two distinguishing features: the first is that it utilizes files in .RTF format as a means for spreading, confusing users in as much as they believe these files to be absolutely safe, often opening them without first administering an anti-virus check. The second is that the Trojan exploits a well-known breach in the Microsoft Word security system, allowing a malefactor to launch malicious code, unbeknownst to a user, immediately following the opening of an infected document. If a computer is not properly patched before the infected RTF file is read, MS Word automatically downloads a template containing the malicious macro-program from a remote Web site without any warning whatsoever. This macro-program extracts an additional utility from the RTF file's binary section. This utility searches the infected computer and creates another .TXT file containing user's Internet access details. At this point, "Goga" starts up the script program that publishes the newly created .TXT file in a Web-site guest book open to the general public. The virus writer is now able to anonymously harvest stolen information from this site.

TROJ_LATINUS.SVR (Aliases: LATINUS.SVR, TrojanDropper.Latinus.14, Backdoor_KF.svr, LATINUS): This is the server component of a backdoor Trojan program that installs itself in the Windows directory of an infected system as MSLAT.EXE. It adds a Windows registry value that loads the Trojan at startup. The server component opens Transfer Control Protocol (TCP) ports 11831 and 29559. It listens to these ports and waits for a connection from the client component. When a connection is established, a remote hacker running the client component gains access to the computer running the server component. This is a remote access Trojan and also a keylogger. It records key strokes and steals passwords that it finds in the system.

TROJ_MEGA.A (Aliases: DDOS/IRCmega, MEGA.A, MEGA): This Trojan launches a Distributed Denial of Service (DDoS) attack using IRC port 6667 and the ping command. It sets the buffer to 65,500 to flood data packets to a target computer. This Trojan also uses mIRC to send messages to its author about the packets sent, the delay, and the failure or successful execution of the Trojan program.

TROJ_MSWORLD.A (Aliases: W32.MsWorld@mm, MSWORLD.A, MsWorld): This Trojan sends itself via Microsoft Outlook to all addresses listed in an infected user's address book. It disguises itself as a Flash movie file, and arrives as an email attachment with one of the following filenames: MWORLD.EXE, MISSWRLD.EXE, or MISSWORLD.EXE. Upon execution, it displays a series of pictures that are supposedly of Miss World contestants. It also modifies the configuration of MAPIUID.INI, sets new time values, and modifies OUTLOOK.PST to increase its file size. Thereafter, OUTLOOK.PST contains embedded data pertaining to various component files being used by the Trojan. Upon the next bootup after infection, this Trojan displays a message and reformats the infected user's C:\ and D:\ drives.

TROJ_WARHOME.A (Aliases: WARHOME.A, WARHOME): This Backdoor Trojan is comprised of a server program and a client program. Its server side installs itself in a target computer, allowing a remote user running the client side to access the infected system. It uses ports 1035 and 23 to establish connection between the client side and the server side. The server program modifies the registry as follows:

KEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Truva = "%VIRPATH%\SERVER.EXE"
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run System-Tray = "SERVER.EXE"
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Microsoft scheduling Agent = "%VIRPATH%\SERVER.EXE"

"%VIRPATH%" is the path where the server program resides. It stays in memory and waits for commands from the client program. The client program prompts for the host name or the Internet Protocol (IP) address of the infected user and thereafter connects to that infected system. The client side can delete files and folders on an infected system.

VBS.Phybre: This is a Visual Basic Script (VBS) Trojan horse. It copies itself into the \Windows\System folder as VBS.Phybre.vbs and modifies the registry so that this file is executed when Windows starts. If the current minute is 39, then the script's payload is activated as follows: A message is displayed that indicates how many times the script has been run and how many times you have been notified of its presence. It attempts to configure the registry so that the script is executed any time that an .htm or .html file is opened on the computer.

VBS.Reset: This is a Visual Basic Script (VBS) Trojan. It modifies the system by turning on user prompting for the running of ActiveX controls and resetting of virus protection in Microsoft Word. When executed, the script modifies the value 1201 in the registry keys:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0

by setting them equal to "1." (Zone "0" references the local computer.) Setting this option to "1" enables prompting for the running of ActiveX controls and plug-ins that are not marked as safe. The script also opens Microsoft Word and turns on the VirusProtection and SaveNormalPrompt options. This means that users will be prompted to enable/disable macros if they are present in a document and prompted if the Normal.dot template file is changed. It also deletes all lines from the Normal.dot (Normal template) file. This has the effect of removing any possible viral macros from the Normal template file.